Upplands Väsby kommun

Rapport: Informationssäkerhet i praktiken
Februari 2023

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Upplands Väsby kommun har EY genomfört en granskning för att testa hur väl kommunens arbete med IT- och informationssäkerhet har kommunicerats till medarbetare i praktiken, exempelvis genom utbildningar och instruktioner. Granskningen syftade till att undersöka om det finns brister i det praktiska arbetet med IT- och informationssäkerhet. Detta genom att bedöma i vilken utsträckning en angripare riskerar att komma åt kommunens IT-miljöer genom angrepp via e-post. De följande revisionsfrågorna har legat till grund för granskningen:

- Hanterar Upplands Väsby kommuns medarbetare hotet från attacker genom falska email, så kallad phishing, på ett ändamålsenligt sätt?
- Har kommunens arbete med instruktioner och riktlinjer kommunicerats på ett sådant sätt att de är kända av medarbetarna?

Granskningen genomfördes från augusti 2022 till februari 2023 och baserades på en simulerad phishing-attack, där kommunens medarbetare uppmanades att klicka på en länk och lämna ut sin användarinformation. EY utformade och genomförde granskningen tillsammans med representanter från kommunen, i syfte att resultatet ska ge så stor nytta som möjligt för verksamheten. Metoden som använts bygger på EY:s etablerade ramverk över hur en organisation arbetar med informationssäkerhet och EY:s beprövade metodik för att genomföra en simulerad phishing-attack. Tre huvudområden analyserades: 1) Mottagare som klickat på länken i e-postmeddelandet, 2) Mottagare som uppgav användarinformation på landningssidan, samt 3) Mottagares medvetenhet kring informationssäkerhet och phishing. Dessa områden jämfördes sedan mot på förhand definierade acceptansnivåer och med vad EY anser är en godtagbar standard i offentlig sektor. Notera att det kan räcka med att en enskild person klickar på länken och eventuellt lämnar sina uppgifter, för att en angripare ska ha uppnått sitt mål och skadan är skedd.

Baserat på genomförd granskning bedömer EY att det finns brister gällande utbildning och medvetenhet inom informationssäkerhet i Upplands Väsby kommun. Granskningsresultatet visar att kommunen ligger på en nivå under det man enligt EY bör förvänta sig av en kommun av denna storlek och karaktär. Slutsatsen bygger på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som kommunen behandlar i dess dagliga verksamhet. I relation till acceptansnivåerna som bestämts i samråd mellan EY och kommunen löper Upplands Väsby kommun en hög risk att utsättas för en fullbordad phishing-attack. Kommunstyrelsen rekommenderas därför att vidta åtgärder för att utveckla relaterade styrdokument och riktlinjer, begränsa antalet rapporteringsvägar för att få en effektiv och samlad rapportering, samt stärka utbildning och medvetenheten hos medarbetarna. En förbättrad motståndskraft mot phishing kan bidra till att förluster av känslig information, negativt rykte eller andra betydande konsekvenser minskar. Baserat på granskningen har EY valt att presentera tre övergripande rekommendationer:

- Dokumentera och tydliggör riktlinjer för informationssäkerhet och phishing.
- Förtydliga föredragna rapporteringsvägar och kommunicera dessa till medarbetarna.

- Införa både teoretiska och praktiska utbildningar inom informationssäkerhet och phishing.

Innehållsförteckning

1. Bakgrund

Upplands Väsby kommun och dess olika nämnder hanterar stora mängder digital information. Detta ger många nya möjligheter i form av effektivare avdelningar, uppföljning och utökad service till medborgare, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrning och arbete bedrivs på ett sådant sätt att informationen är tillgänglig, riktig, har tillräckligt starkt skydd samt är spårbar.

Kommunens revisorer har identifierat risker relaterat till kommunens övergripande arbete med IT- och informationssäkerhet. Revisorerna har därför valt att genomföra en granskning för att testa hur väl kommunens riktlinjer och rutiner med IT- och informationssäkerhet har kommunicerats till medarbetarna i praktiken.

En sådan granskning genomförs genom att EY simulerar en attack där falska email skickas ut till medarbetarna, en så kallad "phishing-attack". Genom ett fullgott informationssäkerhetsarbete bör medarbetarna kunna identifiera ett sådant angrepp och veta hur de ska agera för att hantera och rapportera den simulerade attacken med bibehållen säkerhet. Genom att analysera hur många som agerade korrekt kan revisorerna få en bild av hur väl utbildning och medvetenhet fungerar i praktiken.

1.1 Phishing

Digitalisering leder till en ökad risk, relaterad till informationssäkerhet. Cyberkriminella aktörer väljer i en hög utsträckning att inte enbart attackera tekniken i en organisation, utan även människorna i den. Ett exempel är social manipulation där de utnyttjar mänskliga svagheter som rädsla och förtroende för att utvinna känslig och skyddsvärd information. Angriparen kan även med social manipulation sprida skadlig kod och därigenom tillfoga en organisation, dess intressenter och samhället stor skada. Under covid-19-pandemin har EY sett en ökning av denna typ av cyberkriminalitet, särskilt genom phishing. Det är svårt att fullt ut skydda en organisation mot phishing-attacker enbart genom tekniska hjälpmedel. Detta innebär att den mänskliga aspekten blir avgörande för att i slutänden säkerställa ett adekvat skydd av en organisations tillgångar och för att uppfylla lagkrav inom informationssäkerhet och integritet.

En fullbordad phishing-attack kan innebära stora konsekvenser för en organisation, både finansiellt och socialt, som ett försämrat anseende och rykte. Det är därmed viktigt att vara proaktiv för att hantera det ökade hotet från phishing. En viktig metod för detta är att hålla medarbetare inom en organisation medvetna om hotet från phishing, och delge dem kunskapen att kunna identifiera falska e-postmeddelanden. Medarbetare bör även ha en tydlig rapporteringsväg att följa för att rapportera misstänkta e-postmeddelanden. Att kontinuerligt genomföra medvetenhetsträning för att medarbetare ska upptäcka och reagera på hotet från phishing är ett alternativ för att hantera riskerna från denna typ av cyberattacker.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om det finns brister i det praktiska arbetet med IT- och informationssäkerhet genom att testa utbildning och medvetenhet hos personalen inom kommunen. Vidare är syftet också att bedöma i vilken utsträckning en angripare riskerar att komma åt kommunens IT-miljöer genom angrepp via e-post.

De följande revisionsfrågorna har legat till grund för granskningen:

- Hanterar Upplands Väsby kommuns medarbetare hotet från attacker genom falska email, så kallad phishing, på ett ändamålsenligt sätt?
- Har Upplands Väsby kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av den testade personalen under den simulerade attacken?

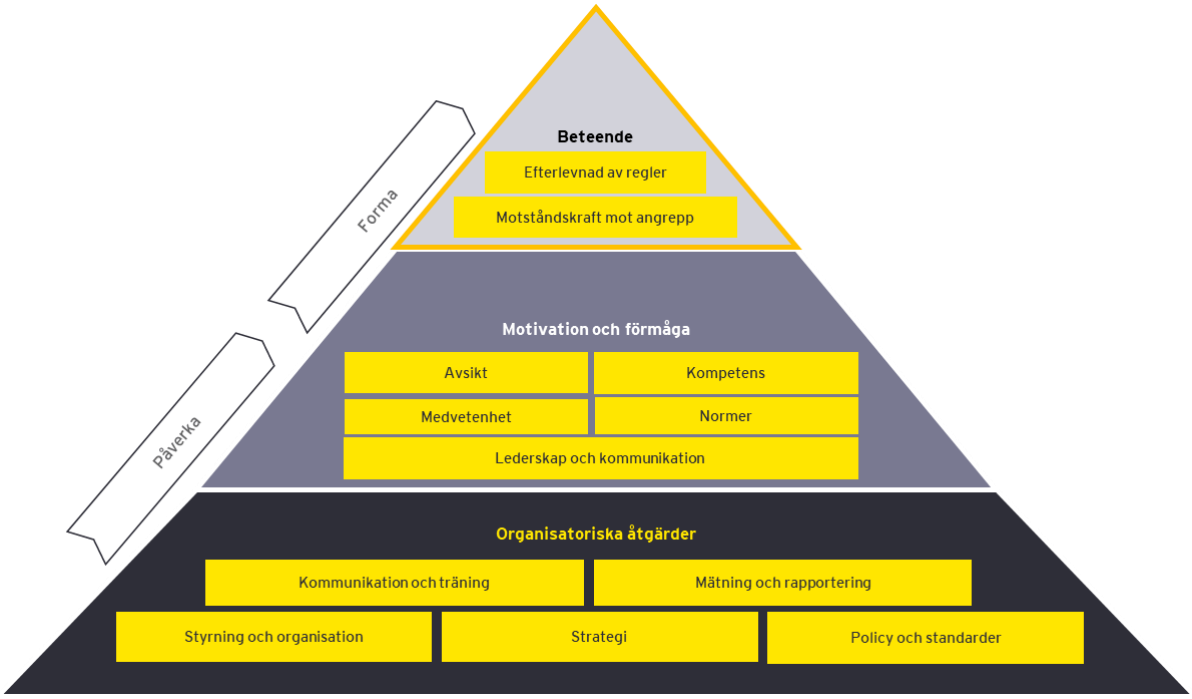
Granskning genomförs enligt god revisionssed inom informationssäkerhetsområdet. Bedömningar görs mot Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk för LIS, som är ett etablerat ramverk i ett stort antal kommuner och inom offentlig förvaltning. Ramverket bygger på den svenska och internationella standarden för informationssäkerhet, ISO/IEC 27000.

1.3 Avgränsningar

Granskningen är avgränsad till att ge en bild hur sårbar kommunen är för attacker riktade mot personalen via e-post. Det ges alltså inte någon helhetsbild av kommunens totala arbete inom IT- och informationssäkerhet utan syftet är ge en mer detaljerad bild av ett begränsat område. Ingen teknisk testning har heller utförts för att granska effektiviteten i kommunens skalskydd, det vill säga hur väl tekniska hjälpmedel fungerar för att identifiera och stoppa falska e-postmeddelanden.

1.4 Metod och genomförande

Granskningen bygger på EY:s etablerade ramverk för hur en organisation arbetar med informationssäkerhet. *Figur 1* nedan visar hur arbetstagarens motivation och förmåga att uppfylla kraven påverkas av genomförda organisatoriska åtgärder. Detta formar i sin tur den enskilda medarbetarens efterlevnad av regler, samt motståndskraft mot angrepp.



Figur 1: EY:s ramverk för bedömning av en organisations informationssäkerhet

Den genomförda granskningen har fokuserat på att analysera beteendet hos kommunens medarbetare genom att utföra en simulerad phishingövning. Övningen testar således främst kommunens, samt de anställdas, motståndskraft mot denna typ av angrepp. Nedan följer en mer detaljerad beskrivning av EY:s metodik för att utföra en phishingövning samt en detaljerad beskrivning av hur övningen genomfördes.

1.4.1 Metod

EY använder en beprövad metodik för att genomföra, och analysera, en simulerad phishingattack. Övningen sätts upp med hjälp av ett verktyg som används för att skicka ut ett e-postmeddelanden till den definierade målgruppen, samt för att samla in data kring det faktiska utfallet. Insamlad information jämförs sedan mot på förhand definierade acceptansnivåer, samt vad EY anser är en godtagbar standard i offentlig sektor. Den information som ligger till grund för granskningen har insamlats av EY i möten med utvalda nyckelpersoner som arbetar med informationssäkerhet inom Upplands Väsby kommun.

För att besvara revisionsfrågorna har EY granskat tre huvudområden enligt nedan:

- **Mottagare som klickade på länken i e-postmeddelandet** – EY har granskat hur många mottagare av det förfalskade e-postmeddelande som klickade på länken till landningssidan inbäddad i e-postmeddelandet. Detta för att få en förståelse för kommunens motståndskraft mot hotet av phishing, samt hur god kunskapsnivån inom kommunens medarbetare är för att kunna identifiera ett e-postmeddelande från en falsk avsändare. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella kan utvinna känslig information, implementera skadlig kod, eller attackera en organisations IT-infrastruktur ökar avsevärt om en mottagare klickar på en skadlig länk eller laddar ner en bilaga i ett e-postmeddelande skickat från en okänd avsändare.

- **Mottagare som uppgav användarinformation på landningssidan** – EY har granskat hur många mottagare av det förfalskade e-postmeddelandet som initialt klickade på länken inbäddad i e-postmeddelandet, för att sedan uppge användarinformation på den förfalskade landningssidan. Detta för att skapa en förståelse för hur stark kommunens motståndskraft är mot angrepp av phishing, samt för att mäta kunskapsnivån hos kommunens medarbetare att kunna identifiera en förfalskad landningssida från en okänd domän. EY bedömer att detta är ett viktigt område att granska då riskerna för att cyberkriminella kan utvinna känslig information och ta sig in i en organisations IT-infrastruktur ökar avsevärt om en medarbetare delar med sig av sin användarinformation som kan leda till en organisations tillgångar.

1.4.2 Genomförande

Övningen har utformats och genomförts av specialister inom IT- och informationssäkerhet från EY, tillsammans med utvalda representanter från Upplands Väsby kommun. De utvalda representanterna från kommunen har givits möjlighet att faktagranska rapporten i syfte att säkerställa att slutsatser grundar sig i korrekta fakta. Nedan följer en ingående beskrivning av respektive huvudmoment för att förbereda, utföra och analysera den simulerade attacken.

1.4.2.1 E-postmeddelande och landningssida

En simulerad phishingattack bygger på att ett e-postmeddelande skickas ut till en utvald målgrupp. E-postmeddelande kan vara utformat på olika sätt baserat på övningens syfte. E-postmeddelandet kan exempelvis innehålla en länk som leder vidare till en internetsida (landningssida), eller inkludera en länk som initierar en nerladdning av en fil. E-postmeddelanden som inkluderar en länk till en landningssida testar vanligtvis hur villiga anställda är att dela med sig av användarinformation som inloggningsuppgifter eller att ladda ner okända filer.

För att bestämma hur e-postmeddelandet skulle utformas hölls inledningsvis möten tillsammans med kommunens representanter. Beslutet föll på att inkludera en länk i e-postmeddelande som hänvisade till en landningssida. På landningssidan uppmanades det att berörd person skulle uppge inloggningsuppgifter (e-postadress samt lösenord) till sitt outlook-konto. För e-postmeddelandet som skickades ut, se *bilaga 1*, samt landningssidan, se *bilaga 2*.

1.4.2.2 Målgrupp och utskick

Målgruppen för en simulerad phishingattack kan variera beroende på övningens syfte. E-postmeddelande kan exempelvis vara riktat mot utvalda avdelningar eller bolag baserat på deras risknivå. E-postmeddelandet kan också skickas ut till samtliga anställda för att på så sätt skaffa sig en övergripande bild av kommunens motståndskraft samt de anställdas medvetenhet.

I samråd med kommunens representanter beslutades det att skicka ut e-postmeddelandet till samtliga 3221 medarbetare inom Upplands Väsby kommun. Innan det faktiska e-postmeddelandet skickades ut hölls ett testmöte där den simulerade attacken testades för att säkerställa att e-postmeddelandet gick igenom skalskyddet och skulle nå fram till mottagarna. Den tekniska genomgången inkluderade behov av vitlistning, spamfilter samt potentiell rate limiting (se *bilaga 4* för definitioner och begrepp) och utfördes den 2

december 2022. Syftet med att koppla bort kommunens tekniska skydd är att på ett kostnadseffektivt sätt testa personalen och inte tekniken. Det bör noteras att inget tekniskt skydd fullständigt kan förhindra ett angrepp genom phishing. Måndagen den 5 december skickades e-postmeddelandet ut till samtliga mottagare och var sedan aktiv i en veckas tid, fram till den 11 december.

1.4.2.3 Rapportering

Att skydda sig mot hotet från en phishingattack är komplicerat och är en samverkan mellan många olika faktorer. En viktig komponent är att effektiva rapporteringsvägar existerar, samt att de anställda är medvetna kring dessa. Åtgärder bör vidtas skyndsamt då hotet är som störst under den initiala tiden efter att e-postmeddelandet mottagits. Det är också av stor vikt att personer som förmodar att de blivit utsatta för angrepp vidtar nödvändiga åtgärder för att ändra inloggningsuppgifter som en angripare kan ha fått tillgång till.

Inom Upplands Väsby kommun finns ingen formell incidentrapporteringsprocess eller rutin för falska e-postmeddelanden. Det finns en hänvisning på intranätet Insidan för användarna, och emellanåt kommer det information på Insidans startsida. Vid mottagandet av ett förmodat falskt e-postmeddelande sker rapportering till stor del till Servicedesk där de gör en första bedömning. Underlaget skickas vidare till IT-drift som undersöker hotet. Det finns ingen officiell hanteringsprocess för detta internt på Servicedesk eller IT-drift och hanteringen kan bero på vem som får frågan på både Servicedesk och IT-drift. Ingen uppföljning eller sammanställning sker.

1.4.2.4 Risknivåer och acceptansnivåer

För att tolka resultaten av en simulerad phishing-attack krävs en förståelse för potentiella risker av en fullbordad attack (risknivåer) och mottagarens relativa benägenhet att acceptera riskerna (acceptansnivåer). Risken för en fullbordad attack kan exempelvis vara mer omfattande för en större kommun då dessa besitter mer känslig information och större finansiell kraft. Det kan också vara skillnader inom en kommun, där vissa avdelningar kan ha mindre risk än andra baserat på typen av verksamhet som bedrivs. Se *tabell 1* för definitioner av risknivåer som EY har använt under genomförd granskning.

Mycket hög risk	En mycket hög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att omgående vidta åtgärder för att åtgärda svagheter i motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Hög risk	En hög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att vidta åtgärder för att utvärdera och åtgärda svagheter i motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Medelhög risk	En medelhög risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att utvärdera och förbättra motståndskraften mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.
Låg risk	En låg risk för, och i samband med, en phishing-attack existerar. Kommunen rekommenderas att arbeta vidare med att kontinuerligt säkerställa en hög motståndskraft mot phishing-attacker. Detta för att undvika finansiella förluster, negativt rykte eller andra betydande konsekvenser.

Tabell 1: Risknivåer för phishing-övning

Innan en simulerad phishing-attack påbörjas är det viktigt att översätta de olika risknivåerna till specifika mätetal anpassade för den aktuella organisationen, vilket kallas för acceptansnivåer. Notera att acceptansnivåerna för andelen mottagare som anger användarinformation på landningssidan generellt sett är lägre än för andelen mottagare som klickar på länken i e-postmeddelandet. Detta då EY anser att risken för att en fullbordad phishing-attack är högre om en cyberkriminell får tillgång till användardata och därmed potentiellt kommunens IT-miljöer. För den simulerade övningen definierades acceptansnivåer i samråd mellan EY och kommunens representanter genom att omvandla risknivåerna till specifika procentandelar, se *bilaga 3*.

1.4.3 Tidsplan

Granskningen genomfördes från augusti 2022 till februari 2023, se *tabell 2* nedan för granskningens tidsplan.

Förberedelser och planering	Augusti 2022
Test och utskick	December 2022
Rapportskrivning och intern kvalitetssäkring	Januari 2023
Justering och färdigställande av rapport	Januari 2023
Avrapportering och slutpresentation	Februari 2023

Tabell 2: Tidsplan

2. Analys

En phishing-attack kan genomföras på många olika sätt vilket kan påverka resultatet och eventuella konsekvenser av attacken. Beroende på vad en cyberkriminell aktör har för målsättning med en attack kan den vara mer eller mindre riktad till specifika personer eller avdelningar inom kommunen. Phishing-attackens utformning påverkar därmed resultatet och bör vägas in i analysen. I följande kapitel analyseras resultatet av den simulerade attack som EY gemensamt med kommunen utformat. Analysen presenteras i tre delar baserat på tre huvudområden: 2.1 Mottagare som klickat på länken i e-postmeddelandet, 2.2 Mottagare som uppgav användarinformation på landningssidan, och 2.3 Mottagares medvetenhet kring informationssäkerhet och phishing.

2.1 Mottagare som klickade på länken i e-postmeddelandet

I detta avsnitt presenteras andelen mottagare som klickade på länken i e-postmeddelandet. Upplands Väsbys kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på kommunens omfattning och riskaptit. *Tabell 3* nedan beskriver de beslutade acceptansnivåerna för andelen mottagare som klickar på länken.

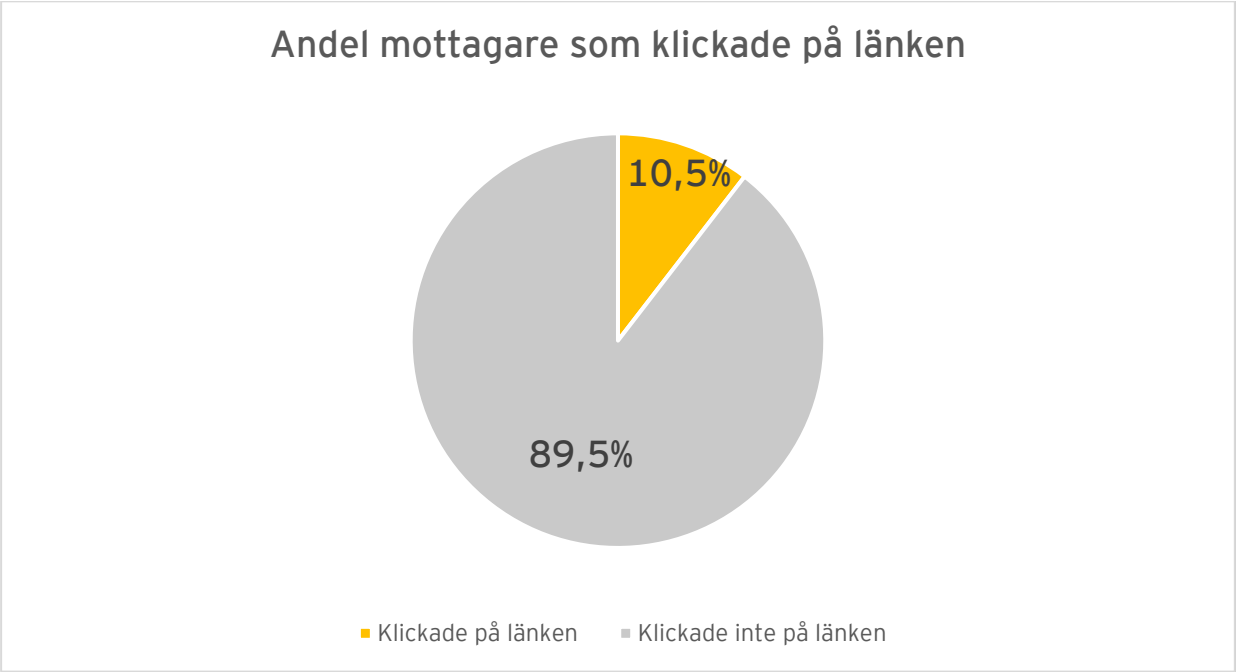
Resultatet av den simulerade attacken för kommunen visar att 10,5 procent av samtliga mottagare klickade på den inbäddade länken i e-postmeddelandet. Resultatet av granskningen visar att enligt de definierade acceptansnivåerna löper Upplands Väsby kommun en hög risk att utsättas för phishing-attacker.

Riskanalys	Acceptansnivå (%)
Mycket hög risk	>15%
Hög risk	10-15%
Medel risk	5-10%
Låg risk	<5%

Tabell 3: Acceptansnivåer för andelen mottagare som klickar på länken

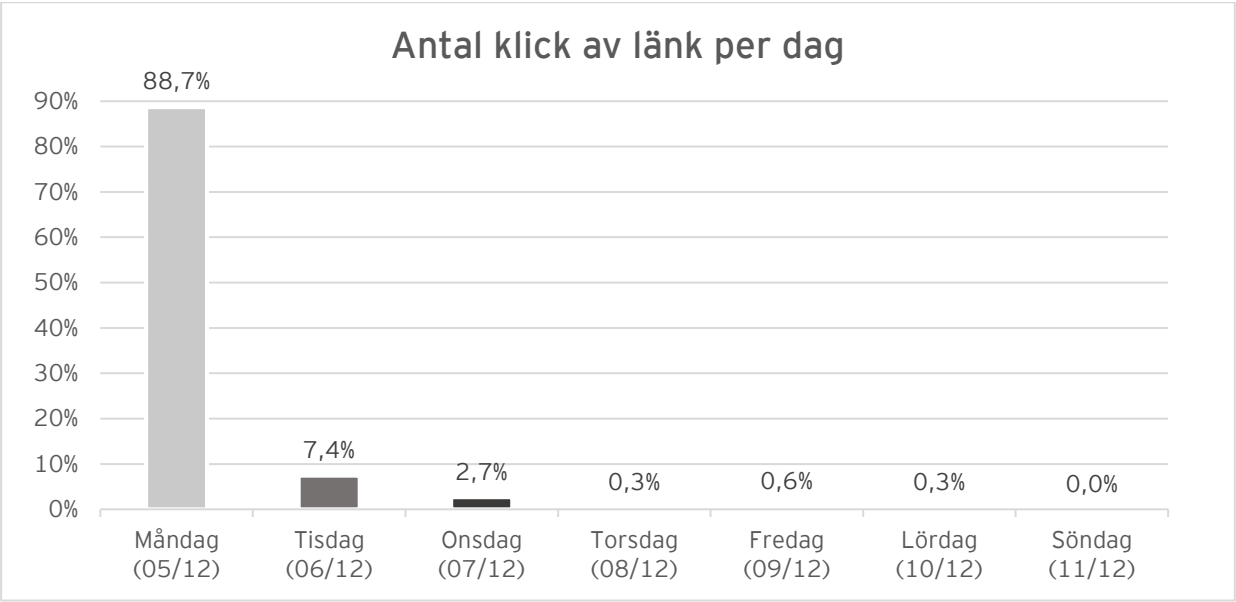
2.1.1 Resultat av simulering

E-postmeddelandet skickades till alla medarbetare inom kommunen. Av 3221 mottagare klickade 337 på länken i e-postmeddelandet, vilket motsvarar 10,5 procent av mottagarna, se *figur 2* nedan. Det här resultatet innebär enligt acceptansnivåerna att Upplands Väsby kommun löper en hög risk för att utsättas för en fullbordad phishing-attack.



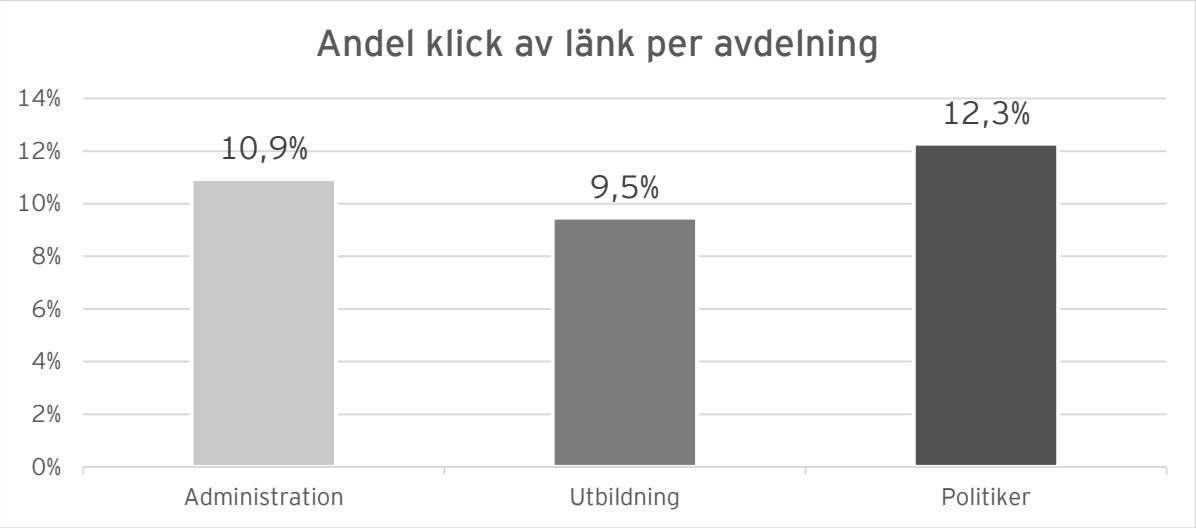
Figur 2: Fördelningen av andel mottagare som klickade på länken i e-postmeddelandet (%).

Simuleringen var aktiv under en vecka. I *figur 3* nedan illustreras andelen klick av länken per dag, där det visualiseras att 88,7 procent av de som klickade på länken i e-postmeddelandet gjorde det under simuleringens första dag. EY noterar att då simuleringen inleddes en måndag, sjönk antalet klick på länken markant under de nästkommande två dagarna, varpå nästintill inga fler klick skedde. Den här trenden är enligt EY förväntad i en simulerad attack då den påkallar omedelbara handlingar av mottagaren.



Figur 3: Andelen klick av länk i e-postmeddelandet under simuleringens aktiva period (%).

Figur 4 visar andelen klick på länken i e-postmeddelandet per avdelning. EY noterar att andelen klick per avdelning generellt är på en hög nivå för samtliga i jämförelse med de på förhand bestämda acceptansnivåerna. EY noterar vidare att politiker hade den högsta andelen mottagare som klickat på länken. Av gruppen politiker klickade 7 av 57 mottagare på länken, vilket motsvarar 12,3 procent. Inom administration klickade 10,9 procent av mottagarna på den inbäddade länken i e-postmeddelandet. Resultatet visade att enligt de bestämda acceptansnivåerna löper dessa avdelningar en hög risk att utsättas för en fullbordad phishing-attack. Inom utbildning låg procentsatsen på 9,5 procent, vilket istället medför en medelhög risk för en fullbordad phishing-attack.



Figur 4: Fördelning av mottagare som klickade på länken per avdelning (%). Notera att andel mottagare som klickat på e-postmeddelandet baseras på antalet e-postmeddelanden som skickades till respektive avdelning.

2.2 Mottagare som uppgav användarinformation på landningssida

I det här avsnittet presenteras andelen mottagare som efter att de klickat på länken i e-postmeddelandet även uppgav användarinformation i form av e-postadress och lösenord på landningssidan. Upplands Väsby kommun hade i samråd med EY på förhand bestämt acceptansnivåer baserat på verksamhetens omfattning. *Tabell 4* beskriver de beslutade acceptansnivåerna för andelen mottagare som uppger användarinformation.

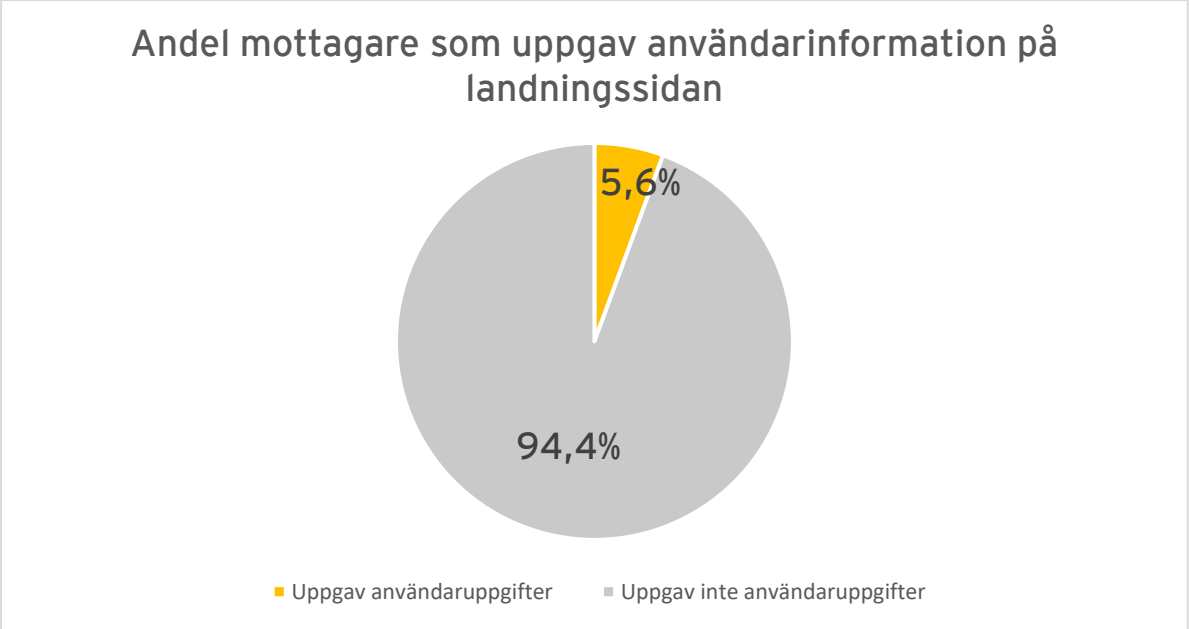
Resultatet av den simulerade attacken för kommunen som helhet visar att 5,6 procent av alla mottagare uppgav sin användarinformation på den förfalskade landningssidan. I relation till de på förhand definierade acceptansnivåerna indikerar resultatet på att Upplands Väsby kommun löper en hög risk att utsättas för en fullbordad phishing-attack.

Riskanalys	Acceptansnivå (%)
Mycket hög risk	>6%
Hög risk	4-6%
Medel risk	2-4%
Låg risk	<2%

Tabell 4: Acceptansnivåer för mottagare som uppger användarinformation på landningssidan

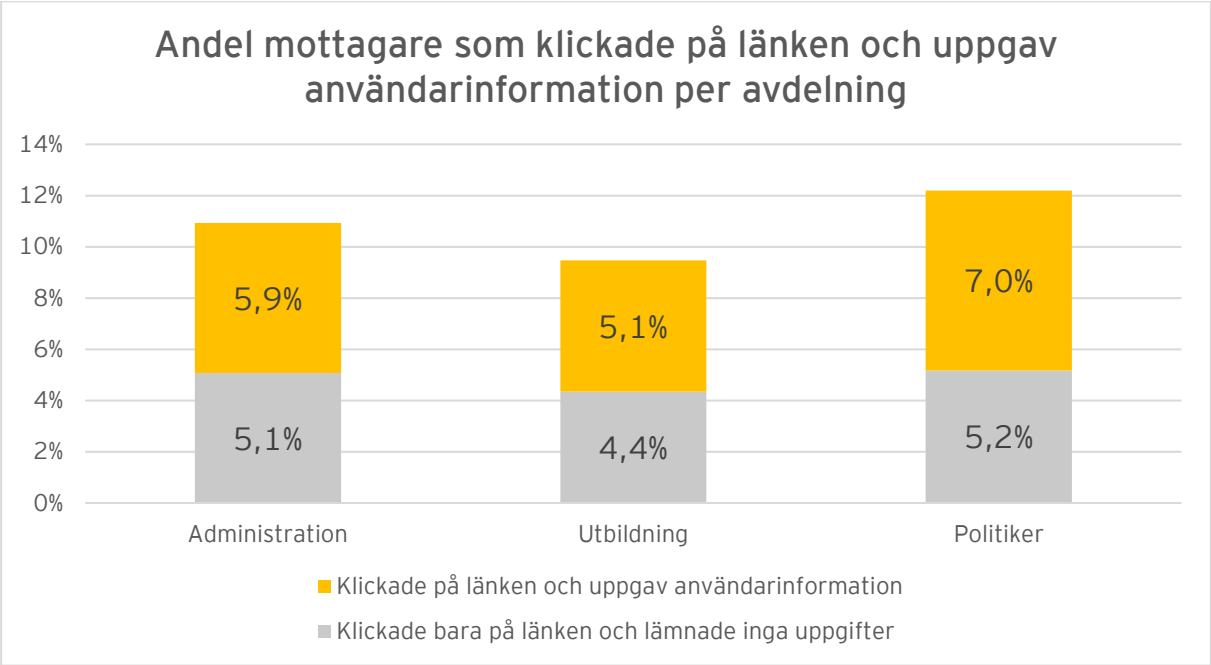
2.2.1 Resultat av simulering

Av det totala antalet mottagare (3221), klickade 181 medarbetare på länken och uppgav sedan sin användarinformation i form av användarnamn och lösenord på landningssidan. Det motsvarar 5,6 procent av alla mottagare, se *figur 6*. I jämförelse med acceptansnivåerna i *tabell 4*, löper därmed Upplands Väsby kommun en hög risk att utsättas för en fullbordad phishing-attack.



Figur 6: Fördelningen av andel mottagare som uppgav användarinformation på landningssidan (%). Resultatet inkluderar kommunen som helhet.

Figur 7 visar andelen mottagare som klickade på länken i e-postmeddelandet i relation till andelen mottagare som, utöver att klicka på länken, även uppgav användarinformation på landningssidan per avdelning. Som tidigare noterat var politiker den grupp där flest mottagare procentuellt klickade på länken. De hade även högst andel mottagare som lämnade användarinformation på landningssidan (7,0 procent), följt av administrationsavdelningen (5,9 procent). EY noterar att baserat på de på förhand bestämda acceptansnivåerna löper samtliga avdelningar en hög risk att utsättas för en fullbordad phishing-attack, varpå politiker löper en mycket hög risk. EY vill även betona att vid en verklig attack kan det räcka med att endast en användare uppger användarinformation för att aktören ska kunna ta sig in i och, i värsta fall, ta kontroll över kommunens IT-miljöer.



Figur 7: Andelen mottagare som bara klickade på länken i relation till mottagare som först klickade på länken och sedan lämnade användarinformation per avdelning (%). Notera att andelen mottagare baseras på antalet e-postmeddelande som skickades till respektive avdelning.

3. Övergripande rekommendationer

Baserat på genomförd analys bedömer EY att Upplands Väsby kommun ligger på en nivå under det man bör förvänta sig av en kommun av denna storlek och karaktär. Bedömningen baseras på den typ av verksamhet som bedrivs och på känslighetsgraden av den information, exempelvis personuppgifter, som kommunen behandlar i dess dagliga verksamhet. Således rekommenderar EY att man inom kommunen vidtar åtgärder för att stärka utbildning och medvetenheten hos medarbetarna och därmed stärker motståndskraften mot phishing-attacker. Detta för att undvika förluster av känslig information, negativt rykte eller andra betydande konsekvenser. I följande avsnitt presenterar EY tre övergripande rekommendationer som bedöms vara mest relevanta för Upplands Väsby kommun.

3.1 Dokumentera och tydliggör riktlinjer för informationssäkerhet och phishing

EY:s ramverk för hur en organisation arbetar med informationssäkerhet indikerar att en organisations motståndskraft styrs av anställdas motivation och förmågor. Motivation och förmågor formas av olika organisatoriska åtgärder som styrning, organisation, kommunikation, utbildning och styrdokument. För att erhålla en god motståndskraft mot cyberattacker krävs således ett övergripande, strukturerat och planlagt arbete med informationssäkerhet.

Resultatet tyder på att medarbetarnas kännedom om hur kommunen arbetar med informationssäkerhet och phishing är relativt låg, vilket EY även bedömer avspeglar sig i resultatet av den simulerade phishing-attacken då cirka 10 procent av samtliga medarbetare klickade på länken i e-postmeddelandet. Under initiala möten med kontaktpersoner från kommunen informerades EY att det i dagsläget saknas dokumenterade, specifika riktlinjer för hur medarbetare ska hantera ett förmodat falskt e-postmeddelande vid en phishing-attack. EY rekommenderar därmed att kommunstyrelsen säkerställer att specifika riktlinjer för phishing fastställs och dokumenteras, samt att dessa riktlinjer inkluderas i befintliga styrdokument för informationssäkerhet inom kommunen.

För att stärka arbetet med informationssäkerhet och phishing inom kommunen rekommenderar EY vidare att styrdokument och riktlinjer tydligt ska kommuniceras och finnas tillgängliga för medarbetarna samt att det finns en tydlig ansvarsfördelning och ett fastställt ägandeskap över dessa dokument. Detta då resultatet från enkäten påvisade att många medarbetare inom kommunen ställer sig relativt osäkra till huruvida de känner till kommunens styrdokument inom informationssäkerhet samt om de är enkla att följa. EY rekommenderar vidare att kommunstyrelsen anordnar utbildningstillfällen gällande innehållet i styrdokument och riktlinjer för att effektivt nå ut till medarbetarna. Det saknas idag en person med utpekat ansvar för informationssäkerhet inom kommunen, EY rekommenderar därmed att en person med tydligt mandat som kan driva dessa frågor tillsätts.

3.2 Förtydliga föredragna rapporteringsvägar och kommunicera dessa till medarbetarna

Det finns olika sätt en organisation kan minska effekterna av en pågående cyberattack genom att underlätta identifiering av attacken, förhindra spridningen och effektivt stoppa den. En förutsättning för att minimera effekterna är att effektiva rapporteringsvägar existerar och att anställda är medvetna om hur och när dessa ska användas. Vid phishing-attacker kan rapporteringen av ett misstänksamt e-postmeddelande möjliggöra att hotet identifieras och att adekvata skyddsåtgärder kan vidtas inom skälig tid. Det är således viktigt att snabbt lyckas identifiera en eventuell phishing-attack för att effektivt motverka attacken eller minimera skadorna. Rapporteringsvägen bör också utvärderas regelbundet och övervakas av ansvariga inom kommunen.

EY rekommenderar således kommunstyrelsen att föredragna rapporteringsvägar fastställs och förtydligas, samt att dessa kommuniceras till samtliga medarbetare inom kommunen. EY anser att man inom kommunen bör begränsa antalet rapporteringskanaler för att få en effektiv och samlad rapportering. Detta eftersom det vid en pågående säkerhetsincident likt phishing är avgörande att kommunens incidenthanteringspersonal snabbt kan bilda sig en förståelse av vad som har inträffat för att effektivt hantera incidenten. Utöver detta rekommenderar EY att det inom kommunen bör finnas väletablerade, dokumenterade rapporteringsvägar tillgängliga för samtliga medarbetare för att säkerställa att kommunen kontinuerligt informeras om potentiella eller pågående säkerhetsincidenter relaterade till phishing-attacker. Under 2022 påbörjades ett internt projekt att skapa en strukturerad process och rapporteringsväg för phishing inom Upplands Väsby kommun.

EY anser vidare att man inom Upplands Väsby kommun arbetar vidare med att kommunicera vikten av att rapportera eventuella säkerhetsincidenter. Kommunikationen bör inkludera tydliga förväntningar och kravställningar på rapportering hos samtliga medarbetare då man misstänker att man blivit utsatt för en phishing-attack. Detta för att öka sannolikheten att fler medarbetare väljer att rapportera en säkerhetsincident relaterat till phishing, men även vet hur de ska gå tillväga för att göra detta.

3.3 Teoretiska och praktiska utbildningar inom phishing

I takt med att mängden cyberattacker mot organisationer har ökat de senaste åren har EY även noterat en markant ökning i antalet phishing-attacker. Detta har bland annat berott på covid-19 och den ökade användningen av digitala verktyg. Anställdas medvetenhet och kunskap om informationssäkerhet blir således allt viktigare för att säkerhetsställa ett adekvat skydd av informationen hos en organisation. Vidare ställs krav på att uppfylla lagar och regleringar om informationssäkerhet och dataintegritet. En phishing-attack kan leda till allvarliga konsekvenser för kommunen, dels genom att utvinna känslig och konfidentiell information, dels genom att implementera skadlig kod på mottagarens enhet.

Den simulerade övningen visade att 10,5 procent av mottagarna klickade på länken i e-postmeddelandet och att 5,6 procent av dessa även uppgav sin användardata på landningssidan. Baserat på resultatet och de satta acceptansnivåerna löper Upplands Väsby kommun en hög risk för att utsättas för en fullbordad phishing-attack. Med anledning av detta rekommenderar EY att utbildningar inom informationssäkerhet och

phishing planeras och följs upp för alla medarbetare inom kommunen. Därtill rekommenderar EY att man inom kommunen undersöker kunskapsbehoven hos medarbetare och därefter inför anpassade utbildningsinsatser.

Specifik utbildning inom phishing syftar till att förbättra medvetenheten och kunskapen om just denna typ av attack genom hela kommunen. Resultatet från granskningen visar även på vilka delar av kommunen som löper störst risk och där riktade utbildningsinsatser kan behövas. EY rekommenderar att kommunstyrelsen säkerställer att utbildningar, inklusive fortsatta phishing-simuleringar, som ger medarbetare kunskapen att kunna identifiera falska e-postmeddelanden, domäner och hemsidor erbjuds för alla medarbetare och övriga personer som har en av kommunen tillhandahållen e-postadress. EY rekommenderar vidare att det inom utbildningarna ska finnas utrymme för interaktiva diskussioner och möjligheter till övning av att jämföra sofistikerade falska e-postmeddelanden med autentiska e-postmeddelanden. Utöver specifika utbildningstillfällen rekommenderas att utbildningsmaterial kontinuerligt sprids till medarbetarna, exempelvis i form av checklistor som medarbetarna kan följa vid misstanke av en phishing-attack.

EY rekommenderar vidare att kommunstyrelsen säkerställer att de teoretiska inslagen följs upp med praktiska övningar som regelbundna tester av säkerhetsmedvetenheten och kunskapen om phishing hos medarbetarna. Detta för att kontrollera effekten av genomförda utbildningsinsatser och för att fortsätta sprida kunskapen inom kommunen. Praktiska övningar syftar till att testa kunskapen som diskuteras under de teoretiska utbildningarna, exempelvis genom att effektivt identifiera ett falskt e-postmeddelande, avsändare eller domän. Det finns olika tillvägagångssätt en kommun kan testa medvetenheten hos anställda, likt interaktivt utbildningsmaterial och nätbaserade simulationer. EY rekommenderar dock att man inom Upplands Väsby kommun fortsätter med uppföljande simuleringar av phishing-attacker för att praktiskt testa medarbetarnas kunskap och medvetenhet, samt för att samla in enhetliga data.

4. Revisionsfrågor

Granskningen har utgått från två revisionsfrågor. Hur väl Upplands Väsby kommun besvarar dessa revisionsfrågor beskrivs nedan.

Färgkod	Förklaring
	Revisionsfråga besvaras ej tillfredsställande
	Revisionsfråga besvarad delvis tillfredsställande
	Revisionsfråga besvaras tillfredsställande

Revisionsfråga	Svar	
▸ Hanterar Upplands Väsby kommuns medarbetare hotet från attacker genom falska email, så kallad phishing, på ett ändamålsenligt sätt?	Baserat på genomförd granskning bedömer EY att Upplands Väsby kommun hanterar hotet av phishingattacker på ett delvis ändamålsenligt sätt. Svaret baserat på den höga andel mottagare som klickade på länken, samt uppgav användaruppgifter, vilket innebär att kommunen löper hög risk att utsättas för en fullbordad attack. Detta visar på ett högt behov att vidta åtgärder för att stärka medvetenheten hos personalen, samt åtgärda svagheter i motståndskraften mot phishingattacker.	
▸ Har Upplands Väsby kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av den testade personalen under den simulerade attacken?	Baserat på genomförd granskning bedömer EY att Upplands Väsby kommuns incidenthanteringsprocess aktiveras på ett ej ändamålsenligt sätt. Slutsatsen bygger på att Upplands Väsby kommun saknar en incidenthanteringsprocess för falska e-postmeddelanden och personalen saknar utbildning för att skydda sig mot en attack. Det ska dock noteras att det i nuläget pågår ett internt projekt för att skapa rutiner och lättillgänglig information vilket kommer att stärka hanteringsprocessen.	

5. Slutsatser

Granskningen syftade till att undersöka det praktiska arbetet med IT- och informationssäkerhet inom Upplands Väsby kommun. Genom en simulerad phishing-attack har EY testat medvetenhet hos personalen. Den genomförda granskningen svarar på följande revisionsfrågor:

- Hanterar Upplands Väsby kommuns medarbetare hotet från attacker genom falska email, så kallad phishing, på ett ändamålsenligt sätt?
- Har Upplands Väsby kommun en incidenthanteringsprocess som aktiveras på ett ändamålsenligt sätt av den testade personalen under den simulerade attacken?

Baserat på genomförd granskning bedömer EY att det finns brister gällande utbildning och medvetenhet inom informationssäkerhet i Upplands Väsby kommun. Resultatet visar att det finns ett behov av att förbättra hanteringsprocessen samt utbildning och medvetenhet inom IT- och informationssäkerhet och phishing, då en stor andel medarbetare inte har tillräcklig kunskap inom området för att kunna identifiera ett falskt e-postmeddelande. Kommunstyrelsen rekommenderas därför att vidta åtgärder för att utveckla och tydliggöra relaterade styrdokument och riktlinjer, begränsa antalet rapporteringsvägar för att få en effektiv och samlad rapportering, och stärka utbildning och medvetenheten hos medarbetarna. En förbättrad motståndskraft mot phishing kan bidra till att förluster av känslig information, negativt rykte eller andra betydande konsekvenser minimeras.

Baserat på resultatet från granskningen har EY valt att presentera följande tre övergripande rekommendationer som man inom Upplands Väsby kommun bör fokusera sitt arbete på framöver:

- Dokumentera och tydliggör riktlinjer för informationssäkerhet och phishing.
- Förtydliga föredragna rapporteringsvägar och kommunicera dessa till medarbetarna.
- Införa både teoretiska och praktiska utbildningar inom informationssäkerhet och phishing.

Stockholm, 2023-02-21

Helena Törnqvist

Partner, EY

Bilaga 1: E-postmeddelande

E-postmeddelande

Ovanlig kontoaktivitet

Servicedesk <servicedesk@upplandvasby.se>

To [redacted]

10:44

Translate message to: English | Never translate from: Swedish | Translation preferences

Hej
Detta är ett automatiserat meddelande för att informera er att det har skett ovanliga inloggningsförsök på ert konto.

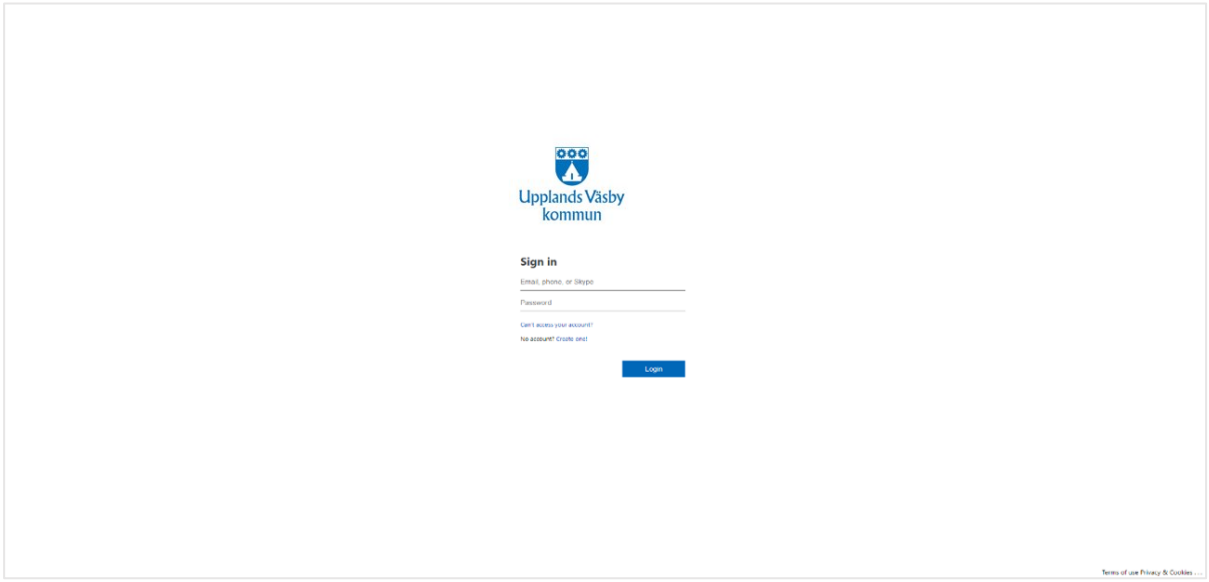
Inloggnings detaljer:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 05/12/2022 07:43 AM (CET)

Om du inte försökt logga in från vänligen logga in och säkra ert konto här: [Länk]

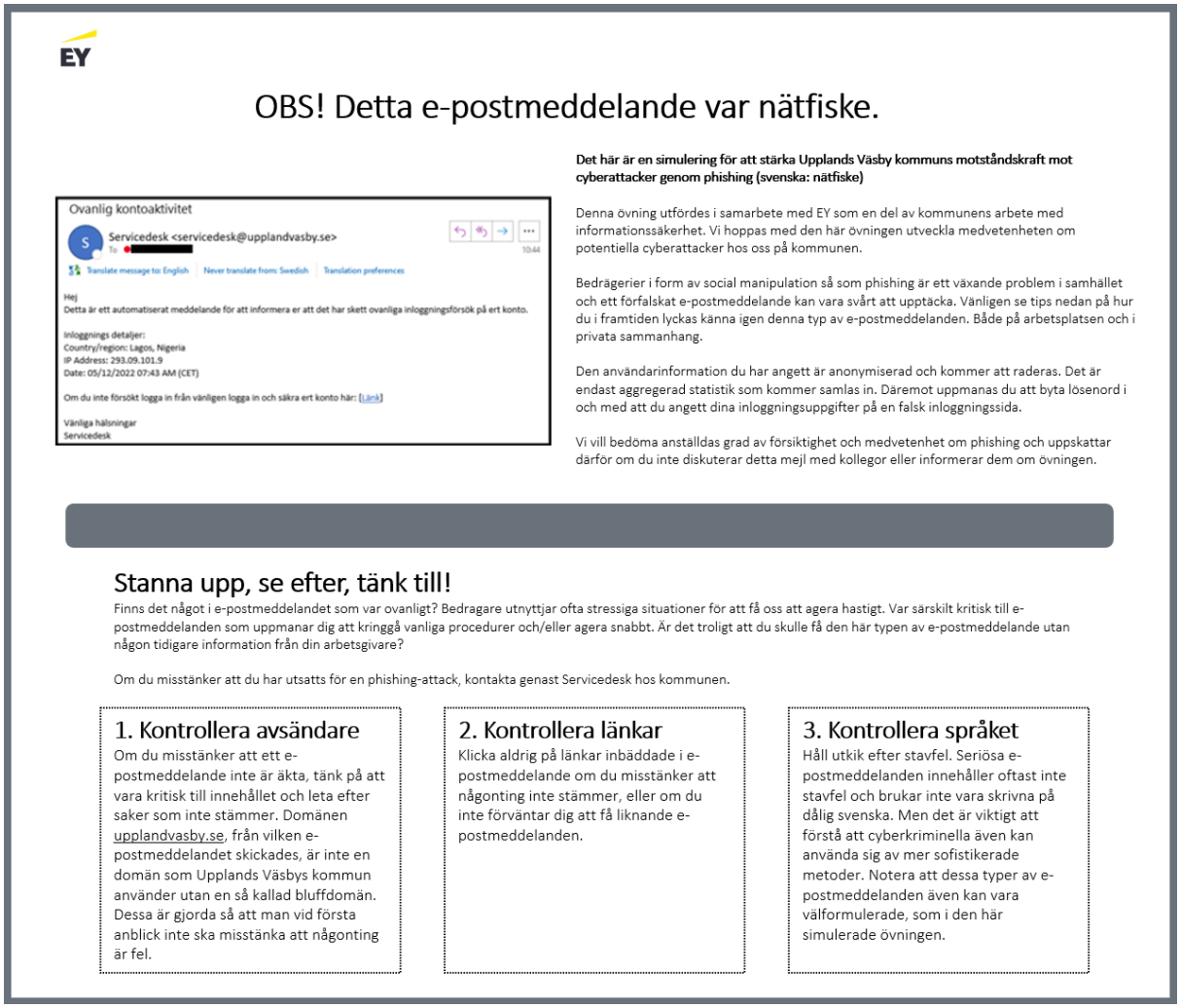
Vänliga hälsningar
Servicedesk

Bilaga 2: Landningssida

Landningssida 1



Landningssida 2



OBS! Detta e-postmeddelande var nätfiske.

Ovanlig kontoaktivitet

Servicedesk <servicedesk@upplandvasby.se>

Translate message to: English | Never translate from: Swedish | Translation preferences

Hej
Detta är ett automatiserat meddelande för att informera er att det har skett ovanliga inloggningsförsök på ert konto.

Inloggnings detaljer:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 05/12/2022 07:43 AM (CET)

Om du inte försökt logga in från vänligen logga in och säkra ert konto här: [Länk]

Vänliga hälsningar
Servicedesk

Det här är en simulering för att stärka Upplands Väsby kommuns motståndskraft mot cyberattacker genom phishing (svenska: nätfiske)

Denna övning utfördes i samarbete med EY som en del av kommunens arbete med informationssäkerhet. Vi hoppas med den här övningen utveckla medvetenheten om potentiella cyberattacker hos oss på kommunen.

Bedrägerier i form av social manipulation så som phishing är ett växande problem i samhället och ett förfalskat e-postmeddelande kan vara svårt att upptäcka. Vänligen se tips nedan på hur du i framtiden lyckas känna igen denna typ av e-postmeddelanden. Både på arbetsplatsen och i privata sammanhang.

Den användarinformation du har angett är anonymiserad och kommer att raderas. Det är endast aggregerad statistik som kommer samlas in. Däremot uppmanas du att byta lösenord i och med att du angett dina inloggningsuppgifter på en falsk inloggningssida.

Vi vill bedöma anställdas grad av försiktighet och medvetenhet om phishing och uppskattar därför om du inte diskuterar detta mejl med kollegor eller informerar dem om övningen.

Stanna upp, se efter, tänk till!

Finns det något i e-postmeddelandet som var ovanligt? Bedragare utnyttjar ofta stressiga situationer för att få oss att agera hastigt. Var särskilt kritisk till e-postmeddelanden som uppmanar dig att kringgå vanliga procedurer och/eller agera snabbt. Är det troligt att du skulle få den här typen av e-postmeddelande utan någon tidigare information från din arbetsgivare?

Om du misstänker att du har utsatts för en phishing-attack, kontakta genast Servicedesk hos kommunen.

1. Kontrollera avsändare

Om du misstänker att ett e-postmeddelande inte är äkta, tänk på att vara kritisk till innehållet och leta efter saker som inte stämmer. Domänen upplandvasby.se, från vilken e-postmeddelandet skickades, är inte en domän som Upplands Väsbys kommun använder utan en så kallad bluffdomän. Dessa är gjorda så att man vid första anblick inte ska misstänka att någonting är fel.

2. Kontrollera länkar

Klicka aldrig på länkar inbäddade i e-postmeddelande om du misstänker att någonting inte stämmer, eller om du inte förväntar dig att få liknande e-postmeddelanden.

3. Kontrollera språket

Håll utkik efter stavfel. Seriösa e-postmeddelanden innehåller oftast inte stavfel och brukar inte vara skrivna på dålig svenska. Men det är viktigt att förstå att cyberkriminella även kan använda sig av mer sofistikerade metoder. Notera att dessa typer av e-postmeddelanden även kan vara välformulerade, som i den här simulerade övningen.

Bilaga 3: Acceptansnivåer

	Mycket hög risk	Hög risk	Medel risk	Låg risk
Andel mottagare som klickar på länken i e-postmeddelandet	>15%	10-15%	5-10%	<5%
Andel mottagare som uppger användarinformation på landningssidan	>6%	4-6%	2-4%	<2%

Bilaga 4: Definitioner och begrepp

Acceptansnivåer: Acceptansnivåer är ett sätt att översätta generella och övergripande risknivåer till aktuella mätetal som går att följa upp och agera på. Acceptansnivåer bör utgå från organisationens eller företagets kontext, dvs. risknivåer och riskaptit.

Cyberattack: En cyberattack är ett samlingsnamn för olika typer av brott som utförs på IT-system. Attackerna kan utföras för att få tillgång till hemlig information, begränsa tillgången till IT-systemen, samt förstöra data eller IT-system.

Domän: Domän, även kallat domännamn, är en beskrivning av ett namn eller en adress på internet. Vanliga exempel på domännamn är det man skriver in i en webbläsare för att komma till en internetsida eller det som kommer efter "@" i en mailadress, exempelvis "google.com" eller "svt.se".

Falsk avsändare: En falsk avsändare är en avsändare som utger sig för att vara någon den inte är, exempelvis genom att imitera kända e-postadresser eller andra avsändare.

Inbäddad länk: En inbäddad länk är en länk man exempelvis bäddar in i en text eller i en bild, vilket innebär att man kan minska transparensen i att en länk existerar eller vart den leder. Processen är vanlig i phishing-attacker då det ökar mottagarnas benägenhet att trycka på länken.

Intranät: Till skillnad från internet som är tillgängligt för alla är ett intranät ofta privat och bara tillgängligt för den organisation eller företag som äger det. Ett intranät är vanligtvis skyddad från omvärlden av en brandvägg och kan bestå av många sammankopplade lokala nätverk.

IT-infrastruktur: IT-infrastruktur är de komponenter inom en organisation som tillsammans används för att producera, hantera, beräkna, hämta och lagra data. Exempel på detta kan vara en databas eller olika servrar.

Landningssida: En landningssida är en internetsida dit en användare hänvisas efter att exempelvis ha tryckt på en länk eller någon annan form av uppmaning.

Phishing: Phishing, på svenska kallat nätfiske, är en metod för cyberkriminella att attackera privatpersoner, företag och organisationer. Metoden går att utforma på olika sätt men går generellt sätt ut på att lura en mottagare att ladda ner en fil, öppna ett dokument eller trycka på en länk via ett sms eller ett e-postmeddelande. Syftet av phishing-attacker är att utvinna konfidentiell information eller att implementera skadlig kod.

Rate limiting: Rate limiting är en engelsk term som beskriver en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen begränsar antalet e-postmeddelanden som kan tas emot samtidigt för att förhindra en eventuell överbelastning.

Spamfilter: Spamfilter, även kallat skräppostfilter, är en inbyggd kontroll som existerar i olika e-postklienter, exempelvis Outlook. Kontrollen sorterar alla e-postmeddelanden som en mottagare tar emot och filtrerar ut de e-postmeddelanden som troligtvis är skräppost.

Vitlistning: Vitlistning är en metod företag och organisationer använder för att kontrollera e-posttrafiken. Detta genom att på förhand definiera vilka e-postadresser som är godkända (vitlistade) och på så sätt tillåta kommunikationen.